2010 North Dakota Users Conference

FRAUD TRENDS AND STRATEGIES

John Carr
Relationship Manager – Public Sector

JPMorganChase

Fraud Definition

Fraud – is defined as unauthorized transaction(s) made with a lost, stolen,compromised or counterfeit card/number.

Types of Fraud

- There are many different “types” of FRAUD
  - Lost/Stolen
  - Non-Receipt
  - Internet
  - Counterfeit/Skimming
  - Stolen/Compromised Number
  - Employee Abuse
  - Account Takeover/True Name Fraud
  - Phishing

2009 Fraud Trends

- Account compromise
- “Phishing” and “Pharming”
- Lost/stolen
- Skimming
- Internet and mail order/telephone order
- International fraud

Current Trends Impacting JPMC

- ❑Gift Cards- counterfeit card used to purchase gift cards from a retail merchant

- ❑Day to Day Living Expenses- not as easily detected in the tools

- ❑Gas Pumps- most common in states with fewer controls

- ❑Counterfeit Fraud- 1st Q, 2010 trended slightly lower that 4th Q 2009, but still remains higher than full year 2009

- ❑Test Merchants- method in which fraudsters test the status of the card

Card Compromise Process

“A compromise can be defined as an incident where card data becomes unsecure or at risk.”

- Notification process begins with the affected party notifying the associations (MasterCard and Visa)
- The associations in turn distribute alerts which notify the issuing banks that they have compromised accounts. The issuers log in to access their data
  - How common is this type of event?
  - When and why do issuers make reissue decisions?

Update

- All affected cards have been closed and re-issued
- Preparations for future events
- Lessons learned

Possible Solutions for Detecting Fraud

- Fraud detection systems
  - Neural network technology
- Counterfeit security measures (CVC/CVV)
- On-line security measures (CVC2/CVV2)

MasterCard/Visa Card Design Security Features

These security features are continuously being improved by the Associations

- Hologram
- Tamper-evident signature panel (CVC2)
- Unique Magnetic stripe encoding (CVC1)

How JPMorgan Chase monitors fraud

Fraud Detection System

- Criteria for queues is based on current fraud trends - these queues can change with unlimited frequency
- Queues can be defined for specific MCC's dollar amounts, states, countries, etc.
- Queues are populated when authorization meets pre-defined criteria

Working the System

- Detection cases are reviewed by security representative
- Account analyzed by history, previous spending patterns, type of transactions, recently issued card
- Accounts may be placed in a referral status until activity is verified
- Cardholder is contacted to validate activity
- Program Admin is contacted if cardholder does not respond – time is of the essence

JPMC Account Review Process

- Review of previous spending history
  - MCC Codes
  - Dollar amount
  - Location
  - Frequency
- Call decision
- Block decision

Investigations and Recovery of Confirmed Fraud

- Affidavit must be returned before recovery efforts begin
- Chargeback Process
  - Mail/Telephone Transactions
  - Internet
  - Card not present at POS

This process may take 30 to 90 days or longer depending on the merchant response

Minimize Risk - North Dakota System's Role

Fraud Prevention

- Cardholder education
- Review of statements
- Prompt notification
  - Lost/Stolen Cards
  - Suspected Fraud
  - Extended Leave
  - Exiting employees

Set realistic limits and MCC restrictions

Secure account number/transactional data

Take advantage of the tools offered in PaymentNet

Review the decline reports regularly

Run the unusual activity analysis report

Run your cardholder list with limits and MCCs

Use transaction list queries to “eyeball” transactions

- Sort by dollar amount and scan
- Sort by merchant name
- Sort by Merchant Category Codes
- You should be the expert on your cardholder’s spending habits

Insurance to protect against Employee Abuse

MasterCoverage or Waiver Liability Insurance

- No cost to the State of North Dakota
- Protects the State against employee misuse of the card

- **Reimburses for unauthorized charges that meet this criteria:**
  - The charges did not benefit the State directly or indirectly
  - The charges occurred between 75 days prior and 14 days after employee termination date
  - Card must be cancelled within 2 business days of such date
  - It is critical that cards are cancelled upon termination of the employee

Keep your cardholders informed

– Best practices – e-mail and outbound calls from JPMC

Phishing is an attempt to gain private information about you and your accounts, most often via e-mail that looks like it is from your financial institution.

It is not JPMorgan Chase's practice to:

- Send e-mail that requires you to enter personal information directly into the e-mail
- Send e-mail threatening to close your account if you do not take immediate action of providing personal information
- Send e-mail asking you to reply by sending personal information
- Send e-mail asking you to enter your user ID, password, or account number into an e-mail or non-secure web page.

You should never reply to, click on, or enter any information if you receive a suspicious e-mail.

Keep your cardholders informed, cont’d.

When receiving a phone call from a JPMorganChase Commercial Card Representative, it is not our practice to ask you to provide:

- Your complete social security number, a representative may ask for the last 4 digits as a verification point
- Card’s expiration date
- CVV or CVV2 from the back of your card

A JPMC Commercial Card Representative may ask you for your account number (usually when returning a message you have left) and it is our practice to verify at least one piece of personal information.

If you are in doubt, do not provide any personal information to the caller. Call the 800 number listed on the back of your card to report the incident.

Top Fraud MCCs*

5411 – Grocery Stores (Super Wal-Mart/Target)

5542 Automated Fuel dispenser

5732 - Electronics

5311 – Department Stores

5310 – Discount Stores

* Subject to change based on fraud trends

Minimizing Risk – We need to work together

- Cardholder communication/education
- PA notification and updates
- Fraud alerts and strategies
- Set appropriate limits and MCC restrictions
- Back-end reporting tools
- Information and best practice sharing
- Prompt notification of status changes

Case Study

Company A	Fraud Losses
2007	$88,000
2008	$86,000
2009	$18,448

- Increase in fraud loss trend detected
- Recommended MCC changes implemented May, 2008
- Over $50,000 in fraud losses avoided in two months
- Common point of compromise identified and reported to Association
- Investigation resulted in confirmation of a merchant breach

Q & A

John Carr
Relationship Manager
(801) 590-1701

Thank you for your time!